ПРИЛОЖЕНИЕ №4

Процедура за проверка на сигурността на информацията, която се въвежда, обработва, съхранява и извежда от ТУМГ

1. Проверка на хардуерната платформа			
Действие	**Очакван резултат/ Критерий за оценяване**	**Констатация /Забележка**	**Съответствие**
Проверка за наличие на възможност за комуникация през хардуерните интерфейси.	Установена липса на възможност за комуникация през хардуерните интерфейси на ТУМГ./Липса на активни хардуерни интерфейси.		
Проверка за наличие на активни комуникационни интерфейси, вградени в ТУМГ.	Установена липса на възможност за комуникация през комуникационните интерфейси./Липса на активни комуникационни интерфейси.		
Проверка за наличие на активна комуникационна подсистема.	Установена липса на възможност за комуникация чрез комуникационната подсистема./Липса на активна комуникационна подсистема, обслужваща различните комуникационни протоколи.		
Проверка за наличие на активни специализирани интерфейси.	Установена липса на възможност за комуникация през специализираните интерфейси./Липса на активни специализирани интерфейси (микрофон/аудио изход/сериен порт/паралелен порт).		

2. Проверка на конфигурацията на операционната система			
Действие	**Очакван резултат/ Критерий за оценяване**	**Констатация /Забележка**	**Съответствие**
Проверка дали са деактивирани ненужни процеси в операционната система на ТУМГ.	Предоставен от страна на Изпълнителя по Договора по обществената поръчка списък с всички процеси в операционната система, които имат отношение към системата на ТУМГ./Липса на процеси, част от операционната система на ТУМГ, които нямат отношение към системата на ТУМГ.		
Проверка за премахнати ненужни firmware пакети и драйвери в ТУМГ.	Премахнати firmware пакети и драйвери в ТУМГ, които управляват хардуерните подсистеми на ТУМГ, нямащи отношение към обезпечаване на изборния процес.		
Проверка за наличие на технически уязвимости в операционната система на ТУМГ. Извършване на оценка за нивото на въздействие на евентуално открити технически уязвимости съгласно Common Vulnerability Scoring System v3.1 (CVSS 3.1) или еквивалентна схема.	Установено неналичие на уязвимости в операционната система на ТУМГ./Липса на уязвимости в операционната система на ТУМГ./ Оценени според нивото на въздействие евентуални уязвимости./Според CVSS 3.1 или еквивалентна система.		
Проверка дали софтуерни компоненти на	Актуализирани софтуерни компоненти на операционната система на ТУМГ с последните кръпки (patches/service		

операционната система на ТУМГ са актуализирани.	packs)за сигурността./Липса на неактулизирани софтуерни компоненти.		
3. Проверка на софтуерната реализация на приложната информационна система			
Действие	**Очакван резултат/ Критерий за оценяване**	**Констатация /Забележка**	**Съответствие**
Компилиране на изходния код на софтуера в специализирана среда с цел тестване за наличието на зависимости в програмния код.	Програмен код с неустановени зависимости./Генерираният бинарен файл на софтуера за ТУМГ следва да бъде изпълним и оперативен по всички заложени критерии за функционалност след компилацията на изходния код в друга среда. Генериран уникален системен криптографски идентификатор (хеш), чрез който се идентифицират произведените софтуерни компоненти вследствие на компилирането.		
Проверка за наличие на технически уязвимости в приложния софтуер на ТУМГ. Извършване на оценка на нивото на въздействие на евентуално открити технически уязвимости, съгласно Common Vulnerability Scoring System v3.1 (CVSS 3.1) или	Установена липса на технически уязвимости в приложната информационна система на ТУМГ./ Оценени според нивото на въздействие евентуални технически уязвимости/според CVSS 3.1 или еквивалентна система.		

еквивалентна система.			
Проверка за възможност за разкриване на вота чрез анализ на данните, записани в електронната избирателна кутия.	Установено неналичие на данни, записани в електронната избирателна кутия, съдържащи идентификационна информация. (За идентификационна информация се считат времеви показатели като дата, час; уникални идентификатори - ID номера, на заявката и други показатели, които могат да идентифицират избирателя)./Липса на данни в електронната избирателна кутия, съдържащи идентификационна информация.		
Проверка на модул за валидация и обобщаване на контролни записки.	Липса на генериран и надеждно съхранен резултатен файл, установен вследствие използване на баркод скенер и софтуерен модул за валидиране.		
4. Проверка на софтуерната реализация на платформата за управление на машинното гласуване			
Компилиране на изходния код на софтуера в специализирана среда с цел тестване за наличието на зависимости в програмния код. Инсталиране и конфигуриране в	Установено наличие на произведена, инсталирана и конфигурирана платформа за управление на машинно гласуване./ Наличие на възможност за автономно персонализиране на всички видове избори съгласно Изборния кодекс.		

специализирана среда.			
Проверка на списък с определени методи и поетапно тестване по предефинирани критерии за съответствие.	Установено наличие на unit tests, които покриват 70% от изходния код на софтуера. Генерирани >70% unit tests./Сравнени резултати от генерираните unit tests с предоставените.		
Проверка за наличие на уязвимости в платформата за управление на машинното гласуване.	Установено неналичие на уязвимости в платформата за управление на машинното гласуване./Липса на уязвимости в платформата за управление на машинното гласуване.		
Извършване на оценка на нивото на въздействие на евентуално открити уязвимости, съгласно Common Vulnerability Scoring System v3.1 (CVSS 3.1) или еквивалентна система.	Оценени според нивото на въздействие евентуални уязвимости/ според CVSS 3.1 или еквивалентна система.		